PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-315998
(43)Date of publication of application : 14.11.2000

(51)Int.CI. H04L 9/14
H04N 7/08
H04N 7/081
H04N 7/167

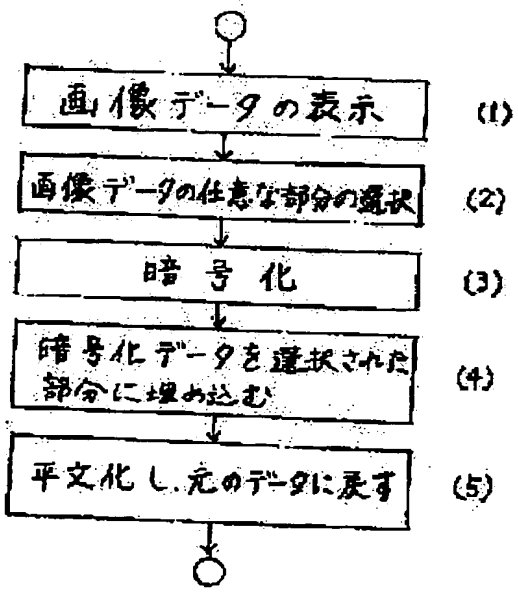
(21)Application number : 2000-100118
(22)Date of filing : 03.01.2000

(71)Applicant : OKANO HIROICHI
OKANO SACHIKO
OKANO JUNKO
OKANO MAKOTO
(72)Inventor : OKANO HIROICHI

(30)Priority
Priority number : 11053071 Priority date : 24.01.1999 Priority country : JP

(54) METHOD AND SYSTEM FOR ENCRYPTING IMAGE

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate the need for other storage area and other file by which partial encryption data of an image is imbedded to an original image and encrypted data are stored.
SOLUTION: An image data display means reads image data and displays the data on a display section (1). A mouse or the like is used for an image data part selection means to select an optional part of an image on the display section (2). An encrypted part is selected, e.g. as a rectangle and their diagonal coordinates may be stored at the end of the original image. Then an encryption means encrypts the selected part (3), and is imbedded to the selected part of the original image data (4). Usually the encrypted data are sent to an opposite party, the opposite party uses a plane text processing means 4 to extract the encrypted part and processes the encrypted part into a plane text and restores the part converted into a plane text to the original data (5). Of course, the data encrypted by itself and stored can be converted into a plane text. In this case, for example, the diagonal coordinates stored at the end of the image are utilized.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２０００－３１５９９８
（Ｐ２０００－３１５９９８Ａ）
(43)公開日　平成12年11月14日(2000.11.14)

(51)Int.Cl.⁷	識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/14	Ｈ０４Ｌ	9/00　６４１	
Ｈ０４Ｎ	7/08	Ｈ０４Ｎ	7/08　Ｚ	
	7/081		7/167　Ｚ	
	7/167			

審査請求　未請求　請求項の数６　書面　（全５頁）

(21)出願番号　特願2000-100118(P2000-100118)

(22)出願日　平成12年1月3日(2000.1.3)

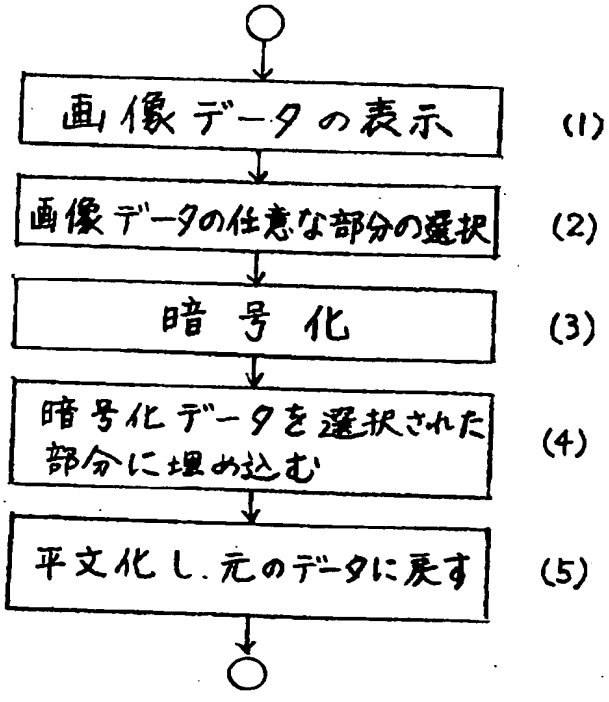
(31)優先権主張番号　特願平11-53071
(32)優先日　平成11年1月24日(1999.1.24)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　591059364
岡野　博一
広島県広島市安佐北区倉掛1丁目8－6
(71)出願人　598160247
岡野　幸子
広島県広島市安佐北区倉掛1丁目8―6
(71)出願人　598160258
岡野　純子
大阪市都島区御幸町1丁目5番8号
(71)出願人　598160269
岡野　誠
京都府京都市左京区一乗寺東杉ノ宮町42
東杉ノ宮ハイツ303号

最終頁に続く

(54)【発明の名称】画像の暗号化方法および装置

(57)【要約】
【課題】　画像の部分暗号を行う。即ち、例えば、対角座標で表される任意の長方形として、画像の一部を選択し、その部分を暗号化し、元の長方形の画像部分に埋め込む。復号に際しては、暗号化された長方形を平文化し、元に戻す。
【解決手段】画像暗号化装置は、メモリを介し画像データ部分選択手段、暗号化手段、平文化手段が接続される。さらに、表示部、補助（外部）メモリ、キーボード、マウス、イメージスキャナ、カメラ等が接続される。



1

【特許請求の範囲】

【請求項１】　下記の（ａ）－（ｄ）の手段を含むことを特徴とする画像データ暗号化装置。

（ａ）表示部と周辺装置に接続されたメモリ手段。

（ｂ）画像データを表示部に表示するため、前記メモリ手段に接続された画像データ表示手段。

（ｃ）前記画像データの任意の部分を指定あるいは選択する、前記メモリ手段に接続された画像データ部分選択手段。

（ｄ）前記選択された部分を暗号化し、前記暗号化された部分を、前記画像データの前記選択された部分に埋め込むための、前記メモリ手段に接続された暗号化手段。

【請求項２】　前記暗号化された部分を取り出し、平文化し、前記平文化された部分を元に戻すための、前記メモリ手段に接続された平文化手段を含むことを特徴とする請求項１記載の画像データ暗号化装置。

【請求項３】　下記の（ａ）－（ｄ）のステップを含むことを特徴とする画像データ暗号化方法。

（ａ）画像データを表示部に表示するステップ。

（ｂ）前記画像データの任意の部分を指定あるいは選択するステップ。

（ｃ）前記選択された部分を暗号化するステップ。

（ｄ）前記暗号化された部分を、前記画像データの前記選択された部分に埋め込む、ステップ。

【請求項４】　前記暗号化された部分を取り出し、平文化し、前記平文化された部分を元に戻すステップを含むことを特徴とする請求項３記載の画像データ暗号方法。

【請求項５】前記ステップ（ｂ）を実行するために、マウスを用いる範囲指定の方法を用いて、前記データの任意の部分を任意の大きさの長方形として選択し、その前記位置として前記長方形の２つの対角座標を記憶するステップを含むことを特徴とする請求項３記載の画像データ暗号化方法。

【請求項６】　下記の（ａ）－（ｄ）のステップを含むことを特徴とする画像データ暗号化方法。

（ａ）画像データを表示部に表示するステップ。

（ｂ）前記画像データの任意の部分を指定あるいは選択するステップ。

（ｃ）前記選択された部分を空白あるいは着色し、暗号化するステップ。

（ｄ）前記暗号化された部分を、前記画像データのファイル内に挿入する、ステップ。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、画像を部分的に暗号化する、画像の暗号化方法および装置に関する。

【０００２】

【従来の技術】暗号化／平文化の変換は、暗号鍵によって制御される暗号アルゴリズムによって実行される。暗号技術は、「辻井、笠原、”暗号と情報セキュリティ”、昭晃堂、１９９０年３月」に詳述されている。代表的な暗号は「U．S．Pat．No．3，958，081　issuedMay　18，1976」に述べられている。これは、DES（「DataEncryption　Standard」，FIPS　PUB，NBS　Jan．1977参照）と呼ばれる。DES暗号は６４ビット単位のデータの暗号を行う。上記の暗号は、対称ブロック暗号と呼ばれるが、これに対して、非対称公開鍵暗号がある。公開鍵暗号として、代表的なRSA暗号は「A　Methodfor　Obtaining　Digital　Signatures　andPublic－Key　Cryptosystems”，Communications　of　the　ACM，Vol．21，No．2，pp．120－126，（1978）」に述べられている。これらの技術は優れており、本発明もこれらの技術を基盤にしている。しかし、これらの技術の使用のみに本発明を限定するものではなく、これらの技術を含めて、色々な種類の暗号技術が本発明に適用できる。

【０００３】なお、「特開昭６３－２１２２７６”ファクシミリ装置”」には、原稿用紙上の送信画像の重要な一部分を暗号化し、その残りをそのままで伝送するファクシミリ装置が記載されている。原稿用紙上の画像データの一部をマーカーで指定し、データ送信時に暗号化する。そして、受信側の出力紙に部分暗号化されたｄｏｔ（点）を元の平文位置に出力する。なお、送信側の暗号処理の詳細な説明及び開示はない。また、通常８ｄｏｔ（点）／mmであり、暗号開始部分が１ｄｏｔ（点）でもずれると、雑音のような出力になるので、紙を入出力媒体として横方向にスキャンしながらデータを読み取ることを考えれば、手書きの指定領域及び暗号部分を読み取るのは非常に困難であって、通常のＦＡＸでは実現困難であり、未完成発明と言える。もちろん、このように紙を情報媒体とする情報伝送技術は、本発明の目的とする電子画像データの伝送を行う情報伝送技術とは異なる技術分野である。例えば、カラー画像データでは、１点をＲ、Ｇ、Ｂ併せて２４ビットで表現する。また、本特許発明者の発明になる、「特願平３－２１５９０９”知的情報処理方法および装置”」には、画像、図形はその一部を長方形でくり抜き、その部分空白で埋め、くり抜いた部分を暗号化して、元の項目にリンクした項目に格納する。この例では、暗号データのためのリンクしたファイルがいる。

【０００４】

【課題を解決するための手段】請求項１記載の画像データ暗号化装置は、下記の（ａ）－（ｄ）の手段を含むことを特徴とする。

（ａ）表示部と周辺装置に接続されたメモリ手段。

（ｂ）画像データを前記表示部に表示するため、前記メモリ手段に接続された画像データ表示手段。

（ｃ）前記画像データの任意の部分を指定あるいは選択する、前記メモリ手段に接続された部分画像データ選択手段。

（ｄ）前記選択された部分を暗号化し、前記画像データの前記選択された部分に埋め込むための、前記メモリ手段に接続された暗号化手段。

請求項３記載の画像データ暗号化方法は、下記の（ａ）－（ｄ）のステップを含むことを特徴とする。

（ａ）画像データを表示部に表示するステップ。

（ｂ）前記画像データの任意の部分を指定あるいは選択するステップ。

（ｃ）前記選択された部分を暗号化するステップ。

（ｄ）前記暗号化された部分を、前記画像データを前記選択された部分に埋め込む、ステップ。

請求項６記載の画像データ暗号化方法は、下記の（ａ）－（ｄ）のステップを含むことを特徴とする。

（ａ）画像データを表示部に表示するステップ。

（ｂ）前記画像データの任意の部分を指定あるいは選択するステップ。

（ｃ）前記選択された部分を空白あるいは着色し、暗号化するステップ。

（ｄ）前記暗号化された部分を、前記画像データのファイル内に挿入する、ステップ。

【０００５】

【作用】画像データをくり抜き、その部分を暗号化し、元の部分に埋め込む。また、くり抜いた部分を空白あるいは着色し、その部分を暗号化したデータを同一ファイル内に挿入する。

【０００６】

【実施例】以下本発明をその実施例を示す図面に基づき詳述する。なお、静止画像、動画像など、および、ホームページ、ワープロ文書、メール、などの電子文書に含まれる画像、および、工業用画像など、全ての画像に適用される。また、全ての暗号技法が適用できる。なお、以下の実施例は本発明の一具体例にすぎず、本発明の技術的範囲を限定するものではない。

【０００７】さて、第１図は基本的な画像の暗号化方法、第２図は画像の暗号化装置である。第２図において、ハードディスク、フロッピィなどの外部メモリ５上の画像ファイル、イメージスキャナ１１、カメラ１２等から画像データが制御部８に入力される。制御部８はマイクロプロセッサからなり、メモリ７に書き込まれている制御プログラムに従ってデータ処理を行う。以下この処理機能を有する仮想的ブロックを想定して説明する。なお、（）内の数字は第１図の手順の番号である。画像データは画像データ表示手段１によって、読み込まれ、表示部６に表示される（１）。表示部６上で、例えば、マウス１０等を用いる画像データ部分選択手段２によって、画像の任意の部分が選択される（２）。暗号化部分は、例えば、長方形として選択し、その対角座標を元の画像の末尾に格納しても良い。つぎに、暗号化手段３によって、選択された部分を暗号化し（３）、元の画像データの選択された部分に埋め込む（４）。通常、暗号化データを相手に送り、その相手は、平文化手段４によって、暗号化された部分を取り出し、平文化し、平文化された部分を元に戻す（５）。もちろん、自分で暗号化し保存したデータを平文化しても良い。この際、例えば、画像の末尾に格納された対角座標を利用する。図３、（ａ）は、元の画像データ、図３、（ｂ）は、部分暗号化データが埋め込まれた画像データの一例である。

【０００８】なお、画像データ部分選択手段２は、単に、対角座標値を入力し、暗号化する長方形を選択する等の方法がある。また、上記、部分暗号処理を、画像暗号化装置に画像を表示した状態で行うことも可能である。また、画像データを、ハードディスク、フロッピィなどの外部メモリに保存したまま、画像データを新しいファイルにコピーしながら、暗号化／平文化の処理を行う等の方法も可能である。また、暗号化部分を示す対角座標等のデータを、元の画像のヘッダーの未使用部分、あるいは、データの末尾など、元の画像ファイル内に、記録しておけば、暗号化／復号化のために必要なデータを別ファイルに添付しなくても良い。勿論、対角座標、暗号鍵、異なる暗号鍵を用いるセキュリティレベルなどを別ファイルに添付する事も可能である。暗号化部分は、従来空白で表示された、横抜き形、または、メモリ上で連続した横抜き形の上下に一行未満のデータ列がある場合も本発明が適用できる。また、プログラムが複雑になるが、さらに、円形、菱形など複雑な形をした暗号化部分も指定できる。例えば、円形部分を選択するには、或点の座標を（ｘ、ｙ）、中心の座標を（Ｘ、Ｙ）とし、半径をＲとし、$(x-X)^2+(y-Y)^2 \leqq R^2$のとき暗号化するようにする。ただし、選択した画像データと暗号化データの大きさが等しいとうまく元の画像に埋め込まれる。このようにすることは容易である。例えば、ＤＥＳ暗号では、暗号化単位（８バイト）の整数倍を選択画像として暗号化すればよい。しかし、暗号化データの方が大きければ、元の画像が欠ける。欠けても実際上画像が損なわれなければ、本発明は有効である。ＲＳＡ暗号でもこのようにできる。さらに、暗号化部分に、異なる暗号鍵を用いる複数のセキュリティレベルを設け、それに応じた暗号鍵／平文化鍵を用いるようにすれば、高度なシステムが構築できる。また、画像データをくり抜き、くり抜いた部分を空白あるいは着色し、その部分を暗号化したデータを同一ファイル内に挿入する、方法も有効である。この場合、着色した色で、複数のセキュリティレベルを表示できる。

【０００９】図４は、画像を含む電子文書の各画像の部分暗号の一例である。テキストデータなどと混在する一つあるいは複数の画像データの部分暗号の場合、暗号鍵（間接的）情報、セキュリティレベル、各画像の部分暗

号データの位置情報等のセキュリティ情報（各画像データの暗号情報）を同一の電子文書内に格納して、暗号化／平文化の処理を行う。なお、このセキュリティ情報を同一の電子文書内にリンクしたファイルに格納してもよい。また、各画像の各セキュリティ情報を各画像のヘッダ部分、各画像の末尾等各画像内に格納しても良い。さらに、各部分暗号化データは、元のデータ部分に埋め込まれてもよく、また、画像データをくり抜き、くり抜いた部分を空白あるいは着色し、その部分を暗号化したデータを同一ファイル内、または、リンクしたファイル内に挿入する等、の方法も有効である。

【００１０】

【発明の効果】以上のように本発明によれば、以下の効果がある。画像の部分暗号データを元の画像に埋め込むので、暗号データを格納するの為の別の記憶領域、ファイルが必要でない。

【図面の簡単な説明】

【図１】基本的な暗号化方法の動作のフローチャートである。

【図２】基本的な暗号化装置のブロック図である。

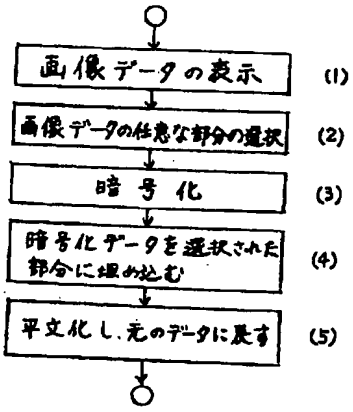
【図３】画像の部分暗号の一例である。

【図４】画像を含む電子文書の各画像の部分暗号の一例

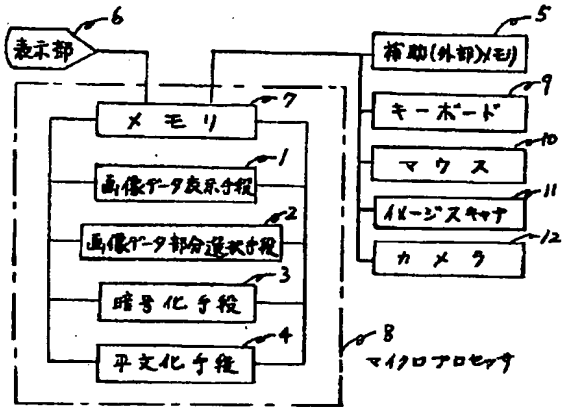
【符号の説明】

1　暗号表示手段段
2　画像データ部分選択手段
3　暗号化手段
4　平文化手段
5　補助（外部）メモリ
6　表示部
7　メモリ
8　マイクロプロセッサ
9　キーボード
１０　マウス
１１　イメージスキャナ
１２　カメラ

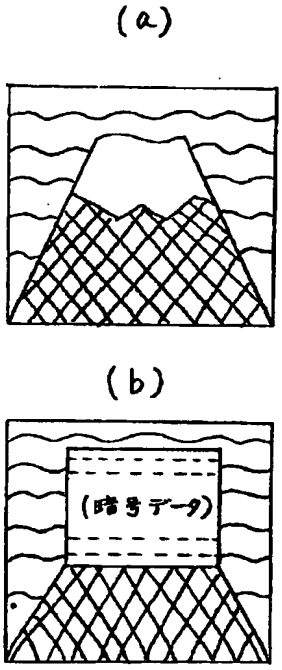
【図１】



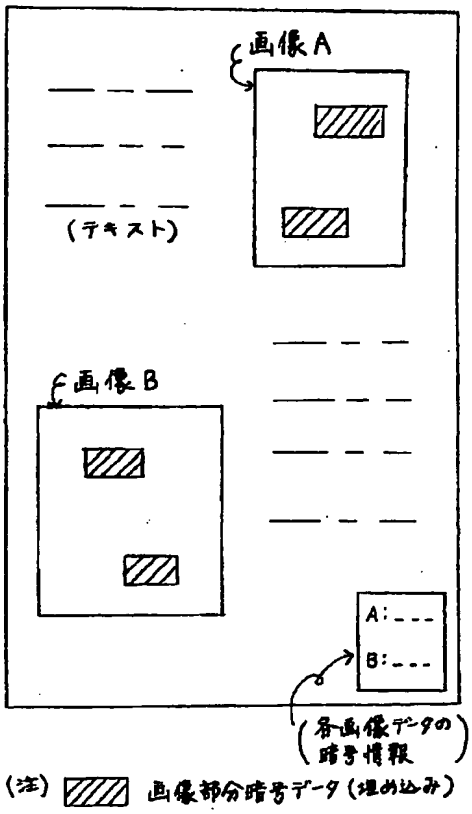
【図２】



【図３】



【図４】



フロントページの続き

(72)発明者　岡野　博一
広島県広島市安佐北区倉掛１丁目８－６